

# A bound on the size of linear codes

**Eleonora Guerrini** (guerrini@science.unitn.it)  
Department of Mathematics, University of Trento, Italy.

**Massimiliano Sala** (msala@bcri.ucc.ie)  
Department of Mathematics, University of Trento, Italy.

---

## Abstract

We present a bound on the size of linear codes. This bound is independent of other known bounds, e.g. the Griesmer bound.

**Keywords:** Hamming distance, linear code, Griesmer bound.

---

## 1 Introduction

The problem of finding a bound for the size of a code is a central problem in coding theory. As regards linear codes, an important (and easy to apply) result is due to Griesmer. In this paper we present a new bound for the size of a systematic code, which is independent of the Griesmer bound when restricted to linear codes. We also show that it is independent of several known bounds on non-linear codes.

For standard definitions and known bounds, the reader is directed to any recent good book on coding theory, e.g. [HP03].

## 2 Our bound

We first recall the result by Griesmer and a few definitions.

Let  $n \geq k \geq 1$  be integers. Let  $\phi : (\mathbb{F}_q)^k \rightarrow (\mathbb{F}_q)^n$  be an injective function and let  $C$  be  $\text{Im}(\phi)$ . We say that  $C$  is an  $(n, k, q)$  **code**. Any  $c \in C$  is a **word**. If  $C$  is a vector subspace of  $(\mathbb{F}_q)^n$ , then  $C$  is a **linear** code.

Let  $\pi : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^k$  be the projection  $\pi(a_1, \dots, a_n) = (a_1, \dots, a_k)$ . We say that  $C$  is **systematic** if  $(\pi \circ \phi)(v) = v$  for any  $v \in (\mathbb{F}_q)^k$ . Clearly, a linear code is systematic.

**Theorem 2.1** (Griesmer bound). *Let  $n$  be the smallest integer such that there exists an  $(n, k, q)$  linear code with minimum distance at least  $d$ . Then*

$$n \geq \sum_{i=0}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor.$$

We are ready to state our result.

**Theorem 2.2** (Bound  $\mathcal{A}$ ). *Let  $n, k, d, i \in \mathbb{N}$ . Let  $n$  be the smallest integer such that there exists an  $(n, k, q)$  systematic code with minimum distance at least  $d$ . If  $n > k > 2$  and  $d \geq 2i + 1 \geq 3$ , then*

$$\binom{k}{i} (q-1)^i \leq \sum_{j=d-i}^{n-k} \binom{n-k}{j} (q-1)^i.$$

*Proof.* We can suppose that  $0 \in C$ . Indeed, if  $0 \notin C$ , let  $\bar{c}$  be a codeword of  $C$ . Then the set  $C' = \{c - \bar{c} \mid c \in C\}$  is a systematic  $(n, k, q)$  code with distance  $d$  and containing the zero vector.

Since  $0 \in C$ , it holds:

$$d(0, c') = w(c') \geq d, \forall c' \in C \text{ such that } c' \neq 0.$$

As a consequence, any word of weight  $i$  in the systematic part has weight at least  $d - i$  in the other  $n - k$  components. Let us consider  $c, c' \in C$  such that  $w(\pi(c)) = w(\pi(c')) = i$ . If  $\pi(c) = \pi(c')$  then  $c = c'$ , since  $C$  is systematic. Moreover, if  $(c_{k+1}, \dots, c_n) = (c'_{k+1}, \dots, c'_n)$ , then  $d(c, c') \leq 2i$  (which implies  $d \leq 2i$ ).

Then, there exists an injective application between the set of vectors  $A$  in  $(\mathbb{F}_q)^k$  of weight  $i$  and the set of vectors  $B$  in  $(\mathbb{F}_q)^{n-k}$  of weight at least  $d - i$ . Clearly,  $A$  contains  $\binom{k}{i} (q-1)^i$  elements and  $B$  contains  $\sum_{j=d-i}^{n-k} \binom{n-k}{j} (q-1)^i$ . Since  $|A| \leq |B|$ , our bound follows.  $\square$

### 3 Remarks

In Table 1 we give some parameters where bound  $\mathcal{A}$  beats the Griesmer bound  $(k_g)$  and other bounds: the Hamming bound  $(k_h)$ , the Levenshtein bound  $(k_l)$  and the Elias bound  $(k_e)$ .

We have not been able to beat the Plotkin bound, but this is not surprising, since the Plotkin bound is experimentally known to be very tight in the tiny range where it can be applied. As regards the Johnson bound, it is very slow to compute and we have been able to search only up to length 140 (compared to  $n = 500$  for the others). In this restricted range we have not been able to beat it. This was expected since the Johnson bound is very good up to small-moderate lengths.

$q$	$n$	$d$	$k_g$	$k_{\mathcal{A}}$	$q$	$n$	$d$	$k_h$	$k_{\mathcal{A}}$	$q$	$n$	$d$	$k_l$	$k_{\mathcal{A}}$	$q$	$n$	$d$	$k_e$	$k_{\mathcal{A}}$
2	20	4	16	15	2	11	4	7	6	2	8	3	5	4	2	7	3	5	4
2	29	7	19	18	2	22	4	17	16	2	10	3	7	6	2	12	3	9	8
2	31	3	28	26	2	30	4	25	24	2	24	5	17	16	2	13	3	10	9
2	45	8	34	32	2	52	4	46	45	2	47	9	32	31	2	47	7	35	34
2	80	15	54	52	2	107	4	100	99	2	66	11	46	45	2	60	7	47	46
2	123	19	89	84	2	127	4	120	119	2	100	4	95	93	2	101	9	81	80
3	6	3	4	3	3	11	4	8	7	3	11	3	9	8	3	10	3	8	7
3	7	3	5	4	3	22	21	3	2	3	23	5	18	17	3	26	3	23	22
3	20	5	15	14	3	29	4	25	24	3	32	4	28	27	3	30	5	24	23
3	40	9	30	28	3	50	46	6	5	3	44	6	37	36	3	73	9	59	58
3	78	15	59	56	3	76	68	9	8	3	50	11	36	35	3	80	11	63	62
3	120	18	97	91	3	120	110	12	11	3	100	13	82	78	3	103	11	85	84
5	10	3	8	7	5	10	8	4	3	5	7	3	5	4	5	16	3	14	13
5	15	5	11	10	5	14	10	6	5	5	13	5	9	8	5	28	5	23	22
5	21	5	17	16	5	30	22	10	9	5	26	6	21	20	5	31	5	26	25
5	53	11	41	40	5	54	50	11	5	5	30	7	24	22	5	75	9	64	63
5	70	19	49	48	5	80	64	21	17	5	60	4	57	56	5	103	11	88	87
5	120	16	101	99	5	131	106	33	26	5	100	3	98	96	5	108	11	93	92

Table 1

Some parameters where bound  $\mathcal{A}$  beats other bounds

## References

- [HP03] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.